Comments of AOL In Connection with the FTC's Report on a System of Rewards for Persons Supplying Information About Violations of the CAN-SPAM Act of 2003

Section 11 of the CAN–SPAM Act requires the Federal Trade Commission to report to Congress on a system for rewarding those who supply information about violations of the Act, including procedures for the Commission to award not less than 20% of any civil penalties collected to the first person that: (i) identifies the spammer; and (ii) supplies information that leads to the successful collection of a civil penalty by the Commission.

America Online, Inc. (AOL) appreciates the opportunity to provide comments to the Federal Trade Commission staff in connection with their study of the CAN-SPAM Act bounty system. AOL applauds the FTC's wide-ranging anti-spam initiatives, and supports cooperative efforts between government and industry that advance the likelihood of enforcement against "outlaw" spammers who engage in the most egregious violations of the CAN-SPAM Act. In AOL's view, the efforts by these "outlaw" spammers to obscure both their identities and the scope of their bulk e-mailing activities are one of the most significant obstacles to enforcement of the Act .

As AOL understands it, the primary purpose of the bounty system is to encourage persons with information that identifies violators of the CAN-SPAM Act to provide that information to the Commission, thereby permitting the government to expedite its enforcement response and at the same time more efficiently expend its resources for tracking down large-scale spammers.

To the extent that a bounty system could enhance government's ability to identity and prosecute the most egregious spam outlaws, such a system might prove a valuable addition to the CAN-SPAM enforcement scheme. Spam outlaws typically use multiple levels of falsification in both their e-mail operations and the financial aspects of their business operations. While both ISPs and government currently expend significant resources attempting to penetrate these techniques of deception, a bounty system offers the FTC the prospect for obtaining new sources of evidence that would help pierce the veil of falsification surrounding spam outlaw activity. In particular, information provided by "insiders" (e.g. former employees, connectivity providers, and business affiliates) in connection with a bounty program might prove a fertile and more rapid path to FTC investigation and enforcement.

Another potential benefit to a bounty system would be to raise public awareness of the problem and its causes, as well as to create a richer, more diverse universe of spam-related complaint data to be analyzed. Consumers who had actually experienced financial loss as a result of responding to fraudulent spam might have a more

direct incentive to provide information to the FTC relating to that loss. Moreover, an increase in the volume of complaints about spam reported to the FTC by consumers – particularly when aggregated into a searchable database[1] -- could improve the analytical tools available to the government for tracking spammers, as well as establishing direct evidence of the specific conduct violating the CAN-SPAM Act (e.g., forged headers, open proxies, dates and volume of mailings).

The potential benefits available under a CAN-SPAM bounty system are, however, likely to be accompanied by significant practical challenges.

Most importantly, the financial incentives in a bounty system to report spam-related complaints might lead to overwhelming volumes of "leads" for the FTC to process. While some of these leads might relate to purely technical information (which might be more susceptible to electronic processing and analysis), others types of leads – such as identity-related tips -- would require significantly more intensive resources for intake and evaluation. Additionally, some of the data reported might be duplicative of readily available public information (e.g., examples of spam messages or leads on transmission methods and identity already available from Usenet group postings and anti-spam activist websites).

Significant challenges would also arise in connection with determining the quality of data provided through a bounty system. Presently, both ISPs and the FTC must make significant efforts to discern the patterns of spam-related activity by large-scale spammers, in order to ensure that their enforcement resources are targeted at the worst actors. The creation of financial incentives for such reporting would create "lottery"-like incentives for reporting of every quantum of evidence relevant to CAN-SPAM enforcement, regardless of the quality of that complaint data, or its materiality to the prosecution of significant CAN-SPAM violations. Moreover, a bounty-driven reporting system might result in an overweighting of investigation of small-scale, "technical" violations of the CAN-SPAM Act by legitimate companies, rather than pursuit of professional spammers using techniques of obfuscation specifically designed to thwart their identification. As a result, investigative resources might be diverted away from enforcement efforts against the largest-scale "outlaw" spammers impacting the greatest numbers of consumers.

Another potential obstacle to the success of a bounty system is the fairly low likelihood of substantial payouts. Based on AOL's experience, only a limited number of outlaw spammers have the sort of wealth or resources that would yield meaningful financial recoveries for whistleblowers. Frequently, the assets that may be available are dissipated immediately by the spammer following the commencement of

---

[1] A bounty system that produced a publicly accessible database of information (or one that could be made available to parties with standing to bring enforcement actions under CAN-SPAM) would be a useful development. Such a database could be used to corroborate information developed through other means, and support enhanced enforcement efforts benefiting consumers.

legal action, or are absorbed by attorneys' fees. Thus, while in the short term the possibility of payouts might stimulate increased reporting to the FTC, in the longer term consumer disillusionment might result in diminution of reporting. Moreover, given the vast amount of publicly available information about spam and spammers, there is also a likelihood of derivative litigation over who is entitled to any bounty that might be available in the event of a successful FTC collection. The cost of such litigation might well exceed the amount of any bounty that is available, even if the program included some equivalent to the "original source" or "public disclosure" doctrines used in the False Claims Act or other whistleblower statutory schemes.

The following additional items might be useful for the FTC to consider in connection with its study of a bounty system:

- the extent to which the use of information derived from a bounty system would be susceptible to additional evidentiary challenges, including impeachment

- the extent to which the incentives to submit evidence in connection with a civil enforcement bounty system would detract from the collection of information leading to criminal prosecution efforts by other federal and state government agencies (independent of a bounty system)

- the extent to which incentives to report spam-related activity in connection with a bounty system would create disincentives for existing anti-spam activists (spamhaus.org, e.g.) to publish investigative information on a pro bono basis, based on fear of "free-riders" exploiting their work

- the nature of the protections from public disclosure (FOIA, e.g.) to be implemented for information submitted in connection with the bounty program

- whether the objective of enhancing lead development might be achieved by means other than a bounty system, such as establishing requirements for the settlement of spam-related enforcement actions that defendants must fully identify all persons they know to be involved in spam-related activity

- whether the promulgation of standards for the quality of information deemed necessary to "identify" a CAN-SPAM Act violator would improve the manageability of a bounty system and the materiality of information provided

AOL hopes that the forgoing proves useful to staff in weighing the challenges and opportunities with a bounty system, and looks forward to the Commission's report.

Charles D. Curran
Assistant General Counsel
America Online, Inc.